

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号
特開2002-164937
(P2002-164937A)

(43)公開日 平成14年6月7日(2002.6.7)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード*(参考)
H 0 4 L	12/66	H 0 4 L 11/20	B 5 K 0 3 0
	12/56		1 0 2 A 5 K 0 3 4
	29/06		1 0 2 D
		13/00	3 0 5 B

審査請求 未請求 請求項の数10 O L (全 21 頁)

(21)出願番号 特願2000-359296(P2000-359296)

(22)出願日 平成12年11月27日(2000.11.27)

特許法第64条第2項ただし書の規定により図面第2図、
5図、6図、8図、9図、10図、11図、12図、15図、23
図の一部は不掲載とした。

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72)発明者 濱 大介

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(74)代理人 100084711

弁理士 齊藤 千幹

Fターム(参考) 5K030 GA19 HA08 HC01 HD03 HD07
KA05 KA13 LB05 MD07
5K034 AA14 BB06 DD03 EE11 HH01
HH02 HH14 HH63

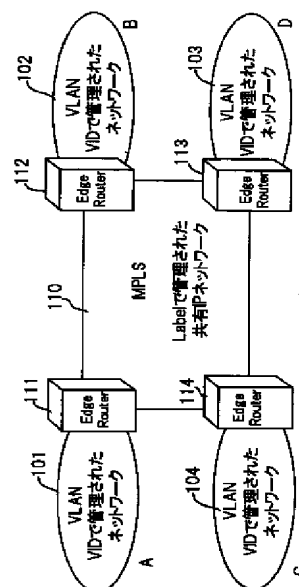
(54)【発明の名称】 ネットワーク及びエッジルータ

(57)【要約】

【課題】 VLANでアクセス系ネットワークを構築し、MP
LS網でコアネットワークを構築するようにして安価な値
段で且つスケール性の高いマルチプロトコルな襟2VPNを
提供する。

【解決手段】 共有ネットワーク上にVPNを形成し、該V
PN内で通信を行うネットワークにおいて、MPLS網110でV
PNのコア網を形成すると共に、VLAN 101~104で該コア
網に対するアクセス網を形成し、MPLS網とVLAN間に、こ
れらMPLS網とVLAN間のインタフェース機能を実行するエ
ッジルータ111~114を設ける。送信側のエッジルータは
VLANから入力するパケットをMPLSのパケットに変換して
MPLS網に送出し、受信側のエッジルータはMPLS網より受
信したMPLSのパケットをVLANのパケットに変換し、該VL
ANパケットを送信側VLANと同一のVPNに属する VLANに向
けて送信する。

本発明のVLANとMPLSの混在ネットワークの概略図



【特許請求の範囲】

【請求項1】 共有ネットワーク上にVPNを形成し、該VPNを介して通信を行うネットワークにおいて、ラベルスイッチ網でVPNのコア網を形成すると共に、VLANで該コア網に対するアクセス網を形成し、ラベルスイッチ網とVLAN間のインタフェース機能を実行する装置をこれらラベルスイッチ網の端に設けた、ことを特徴とするネットワーク。

【請求項2】 前記インタフェース装置は、ラベルスイッチ網であるMPLS網の端に設けられたエッジルータであり、送信側のエッジルータはVLANから送出されるパケットをMPLSのパケットに変換してMPLS網に送出し、受信側のエッジルータはMPLS網より受信したMPLSのパケットをVLANのパケットに変換し、該VLANパケットを送信側VLANと同一のVPNに属するVLANに向けて送信する、ことを特徴とする請求項1記載のネットワーク。

【請求項3】 前記エッジルータはVLANのパケットに含まれるVLAN識別子(VID)とMPLSのパケットに含まれるVPNラベルの対応を記憶するテーブルを備え、送信側エッジルータはVLANパケットのVIDに応じたVPNラベルを求め、該VPNラベルを有するMPLSパケットを生成してMPLS網に送出し、受信側エッジルータはMPLS網より受信したMPLSパケットに含まれるVPNラベルに応じたVIDを求め、該VIDを有するVLANパケットを生成し、該VIDが示すVLANに送出する、ことを特徴とする請求項2記載のネットワーク。

【請求項4】 前記エッジルータは、受信側のエッジルータに向けてMPLSパケットを送出する経路を決定するルート決定部、ルート決定部により決定された経路を特定する転送用ラベルを受信側エッジルータのアドレスに対応させて記憶するテーブルを備え、送信側エッジルータは、パケットの宛先MACアドレスに応じた受信エッジルータを求め、該テーブルより受信エッジルータに応じた転送用ラベルを求め、前記VPNラベル及び転送用ラベルを含むMPLSパケットを生成してMPLS網に送出する、ことを特徴とする請求項3記載のネットワーク。

【請求項5】 前記VPNを構成するVLANに接続するエッジルータはそれぞれ、該エッジルータに接続するVLAN構成装置のアドレスとエッジルータのアドレスを組にして前記他のエッジルータに送出し、各エッジルータは受信情報に基づいてレイヤ2ルーティングテーブルを作成し、送信側エッジルータは、該レイヤ2ルーティングテーブルより前記パケットの宛先に応じた受信エッジルータを求める、ことを特徴とする請求項4記載のネットワーク。

【請求項6】 共有ネットワーク上にVPNを形成し、MPLS網で該VPNのコア網を形成し、VLANで該コア網に対する

アクセス網を形成するネットワークにおけるエッジルータにおいて、

VLAN識別子(VID)とVPN識別子であるVPNラベルの対応を記憶する手段、

前記対応関係を用いてVLANから送出されるパケットに含まれるVIDに応じたVPNラベルを求め、該VPNラベルを含むMPLSパケットを生成してMPLS網に送出するMPLSパケット生成部、

を備えたことを特徴とする送信側エッジルータ。

【請求項7】 前記エッジルータは更に、受信側のエッジルータに向けてMPLSパケットを送出する経路を決定するルート決定部、

ルート決定部により決定された経路を特定する転送用ラベルを受信側エッジルータに対応させて記憶する転送用ラベル記憶部、

を備え、前記MPLSパケット生成部は、パケットの宛先MACアドレスに応じた受信エッジルータを求め、該転送用ラベル記憶部より受信エッジルータに応じた転送用ラベルを求め、前記VPNラベル及び転送用ラベルを含むMPLSパケットを生成する、ことを特徴とする請求項6記載のエッジルータ。

【請求項8】 前記MPLSパケット生成部は、前記VPNを構成する他のVLANに接続するエッジルータより送られてくる該エッジルータのアドレスと該エッジルータに接続するVLAN構成装置のアドレスとの組み合わせ情報に基づいてレイヤ2ルーティングテーブルを作成し、該レイヤ2ルーティングテーブルよりパケットの宛先に応じた前記受信エッジルータを求める、ことを特徴とする請求項7記載のエッジルータ。

【請求項9】 共有ネットワーク上にVPNを形成し、MPLS網で該VPNのコア網を形成し、VLANで該コア網に対するアクセス網を形成するネットワークにおけるエッジルータにおいて、

VLAN識別子(VID)とVPN識別子であるVPNラベルの対応を記憶するテーブル、

前記テーブルを用いてMPLS網より入力するパケットに含まれるVPNラベルに応じたVIDを求め、該VIDを含むVLANパケットを生成してMPLS網に送出するVLANパケット生成部、

を備えたことを特徴とする受信側のエッジルータ。

【請求項10】 共有ネットワーク上にVPNを形成し、MPLS網で該VPNのコア網を形成し、VLANで該コア網に対するアクセス網を形成するネットワークにおけるエッジルータにおいて、

VLAN識別子(VID)とVPN識別子であるVPNラベルの対応を記憶するテーブル、

前記テーブルを用いてVLANより入力するパケットに含まれるVIDに応じたVPNラベルを求め、該VPNラベルを含むMPLSパケットを生成してMPLS網に送出するMPLSパケット生成部、

前記テーブルを用いてMPLS網より入力するパケットに含まれるVPNラベルに応じたVIDを求め、該VIDを含むVLANパケットを生成してMPLS網に送出するVLANパケット生成部、
を備えたことを特徴とするエッジルータ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はネットワーク及びエッジルータに係わり、特に、共有ネットワーク上にVPN (Virtual Private Network)を形成し、該VPN内で通信を行うネットワーク及び共有ネットワーク上にVPNを形成し、ラベルスイッチ網で該VPNのコア網を形成し、VLAN (Virtual LAN)で該コア網に対するアクセス網を形成するネットワークにおけるエッジルータに関する。

【0002】

【従来の技術】社内のネットワーク（イントラネット）を構築するためには、各地に散在する本社、営業所、支店、工場、研究所等を相互に接続する必要がある。又、本格的な国際化の時代を迎え、イントラネットは日本国内だけで閉じないで、広く海外拠点まで接続する必要性が生じている。このようにイントラネットが広域化すると、離れたオフィスにいてもあたかも本社のオフィスにいるのと同じようなシステム環境を実現する要求が生じ、VPN (Virtual Private Network)技術が開発され広く採用されている。VPNとは共有ネットワーク（インターネット等の広域網）上に設けられ、ユーザが共有ネットワークの利用を意識することなく利用できる仮想の私設網であり、アクセスサーバ、WANルータ、VPN専用装置等を利用してWAN上に構築される。VPNを構築する技術には、IEEE802.1QのVLAN (Virtual LAN)による方法、IPsecによる方法、MPLS (Multiprotocol label Switching)による方法などがある。

【0003】VLAN (仮想LAN)は、ネットワークに接続された機器をその物理的な配線や構成に関係なくグループ化するもので、グループ化はレイヤ2にあたるMACフレームが到達する範囲内において行われる。フレームの送受は同一グループ内で行われ、フレームのブロードキャストも同一グループ内で行われる。異なるVLANグループ間の通信はレイヤ3における中継動作を行うルータを介さなければならない。VLANを実現する方式には、(1)ポートベースVLAN、(2)MACアドレスデータベースVLAN、(3)ポリシーベースVLANなどがある。このうち、ポートベースVLANは、スイッチングハブ (switching HUB)上の物理ポート単位で静的にVLANグループを形成する方式であり、又、MACアドレスデータベースは端末が持つMACアドレスをベースにしてVLANグループを形成するもので、受信パケット内の発信元MACアドレスに基づいて該当するVLANグループを認識する。

【0004】図18はポートベースVLANの構成例であり、スイッチングハブSHBの複数LANポートP1～P6にそれ

ぞれパソコン等の端末が接続されている。LANポートP1～P3はグループ1に属し、LANポートP3～P6はグループ2に属する。グループ1の所定端末から送信されたブロードキャストフレームはグループ1内の端末のみにブロードキャストされ、グループ2の端末から送信されたブロードキャストフレームはグループ2内の端末のみにブロードキャストされる。又、フレームの送受は同一グループ内で行われ、異なるVLANグループ1、2間の通信は図示しないルータを介さなければならない。以上より、グループ化以前にはブロードキャストフレームを全端末に中継していたのがグループ内のみに中継するだけで良くなり、ネットワークの負荷を軽減できる。しかも、他のグループにフレームは送信されないためセキュリティを維持することができる効果が発生する。

【0005】VLANではLANポートP3のように複数のグループに属するように重複して設定することができる。又、グループ化は1台のスイッチングハブに限らず、図19に示すように複数のスイッチングハブSHB1～SHB3に属するポートをグループ化することもできる。すなわち、各スイッチングハブSHB1～SHB3のポートP1～P3をグループ化し、各グループに固有の識別子であるVLAN ID (VID: Virtual LAN Identifier)を付与すると共に後述するタグ方式を採用することにより複数の装置にまたがった複数のVLAN (VLAN1～VLAN3)を構成することができる。これにより、同一のVLANに属する端末は設置場所に依存することなく、あたかも同一の物理ネットワークに接続しているかのように通信することができる。

【0006】ここでタグ方式とは、IEEE802.1Qにより標準化された手法である。タグ方式では、VIDをMACフレームにタグという形で付与し、このタグをパケットと共にMACフレームで運ぶ。タグ付きMACフレームを受信したL2スイッチ (スイッチングハブ)はタグの内容を解析し、そのVLANに属する適切なポートに中継処理する。

【0007】図20はVLAN (IEEE802.1Q)のMACフレームフォーマットであり、M1はMAC宛先アドレス (MAC DA)、M2はMAC発信元アドレス (MAC SA)、M3はタグ、M4はタイプ、M5はIPパケット (IPヘッダ/TCPヘッダ/データ部)である。タグM3は4バイトで構成され、①TPID (Tag Protocol Identifier)、②ユーザプライオリティ、③CFI (Canonical Format Indicator)、④VID (Virtual LAN Identifier)、⑤length、⑥RIF (Routing Information Field)を有している。TPIDの値は16進数で81-00 (IEEE802.1Qタグタイプ)に固定されている。ユーザプライオリティはフレームの優先順位を3ビットで表現したもの、CFIはタグヘッダにおけるRIF fieldの有無を示すもの、VIDは12ビット構成のバーチャルLAN識別子であり、 $2^{12}=4096$ 個のVIDを指定することができる。

【0008】図21はVLANの実現例であり、PC1～PC4はパソコン端末、SHB1はポートP1、P2にパソコン端末PC1、PC2が接続された第1のスイッチングハブ、SHB2はポ

ートP1、P2にパソコン端末PC3、PC4が接続された第2のスイッチングハブ、SHB3はポートP1、P2に第1、第2のスイッチングハブSHB1,2が接続された第3のスイッチングハブ、RTは第3のスイッチングハブSHB3のポートP3に接続されたルータである。第1、第2のスイッチングハブSHB1,2はそれぞれポートP3を介して第3のスイッチングハブSHB3と接続している。

【0009】第1、第3のパソコン端末PC1,PC3はVID=10の第1のVLANを構成し、第2、第4のパソコン端末PC2,PC4はVID=20第2のVLANを構成し、又、スイッチングハブSHB1～SHB3の各ポートP1～P3は図中のVID値で示すようにグループ化されている。尚、2つのVID値を有するポートは2つのグループに属するものである。パソコン端末PC1からパソコン端末PC3にパケットを送信する場合、パソコン端末PC1はヘッダにパソコン端末PC3のMACアドレスを宛先アドレスとして有するパケットを送出する。該パケットをポート1より受信した第1スイッチングハブSHB1は、該ポート1の属するVLANのVID(=10)を予め設定されているテーブルより求め、該VID=10を含むタグを受信パケットに付加してVID=10のポートP3より送出する。以後、該タグ付きパケットは第3スイッチングハブSHB3のポートP1,P2を介して第2スイッチングハブSHB2に送信される。第2スイッチングハブSHB2はタグ付きパケットが到来すれば、タグを外してVID=10のポートP1よりパソコン端末PC3に送信する。

【0010】一方、パソコン端末PC1から別グループのパソコン端末PC4にパケットを送信する場合、パソコン端末PC1はレイヤ2ヘッダにルータRTのMACアドレス(レイヤ2アドレス)を宛先アドレスとして有し、レイヤ3ヘッダ(IPヘッダ)にパソコン端末PC4のレイヤ3アドレス(IPアドレス)を有するパケットを送出する。該パケットをポート1より受信した第1スイッチングハブSHB1は、該ポート1の属するVLANのVID(=10)をテーブルより求め、該VID=10を含むタグを受信パケットに付加してVID=10のポートP3より送出する。第3スイッチングハブSHB3は該受信パケットをそのままVID=10を有するポートP3より送出する。ルータRTはパケットを受信すれば、宛先のレイヤ3アドレスを参照してVID値を10から20に変更し、かつ、パケットの宛先MACアドレスをパソコン端末PC4のMACアドレスに変更して該パケットをポートP1より送出する。以後、該タグ付きパケットは第3スイッチングハブSHB3のポートP3,P2を介して第2スイッチングハブSHB2に送信される。第2スイッチングハブSHB2はタグ付きパケットが到来すれば、タグを外してVID=20のポートP2よりパソコン端末PC4に送信する。以上のVLANによれば、企業の情報システム(イントラネット)の既存資産を保存しながら、次世代LANへの基盤を柔軟に構築でき、ネットワーク管理/運用を統合して合理化を図ることができる。

【0011】VPNを構成する方法としてMPLS(Multiprotocol

label Switching)による方法がある。MPLSは、コネクションという概念のないIP網にパス(仮想的な通信路)の概念を持ちこむプロトコルである。MPLS網は、IPパケットにコネクションを識別するための新しいフィールド「label」を追加し、ネットワーク上のルータはlabelフィールドのlabel値をpop、pushまたはswapしてIPパケットを伝搬する。このMPLSによれば、IPのコネクション型サービスを提供でき、しかも、コネクション毎にセキュリティを確保でき、更に、専用線の代替手段となるIP専用線サービスをIP網で効率良く提供することができ、非常にscalabilityの高い方法である。又、MPLSを使ってVPNを構築する方法がRFC2547BGP/MPLS VPNsとして公開されており、このRFC法により、インターネットワーク上にIP VPNを構成することが出来る。

【0012】MPLSは、レイヤ2とIP層の中間に位置付けられる。通常のルータはIPパケットのIPヘッダを参照して転送処理を実行するが、MPLS対応ルータはIPヘッダを参照せず、IPヘッダとL2ヘッダ間に設けられるlabelに基づいて転送処理する。図23はMPLSの説明図であり、1～5はMPLS用ルータであり、MPLSルータ1、5はMPLS網の外部と接続するエッジルータを構成し、MPLSルータ2～4はMPLS網内のコアルータを構成する。エッジルータ1には送信側の端末装置がLAN等を介して接続され、又、エッジルータ5にIPアドレス10.1.100.0/24を有する宛先の端末装置がルータ、LANを介して接続されている。両端末間で通信を行うものとする、予め、両端末が接続されたエッジルータ1、5間にLDP(label distribution protocol)に従ってLSP(label switched path)がlabelを用いて設定され、このLSPを形成する各MPLSルータ1～4にはラベルテーブル1a～4aが作成される。

【0013】かかる状態において、送信側端末装置よりIPパケットを含むMACフレームが入力すると、エッジルータ1はテーブルを参照してMACフレームにMPLSのヘッダであるshimヘッダ(後述する)を付加し、該shimヘッダのlabel fieldにlabelとして「39」を付加し(push)、次のMPLSルータ2に向けて送信する。MPLSルータ2はテーブル2aを参照してlabel「39」をlabel「37」に付け替え(swap)、次のMPLSルータ3に向けて送信する。MPLSルータ3もテーブル3aを参照してlabel「37」をlabel「36」に付け替え(swap)、次のMPLSルータ4に向けて送信する。同様に、MPLSルータ4はテーブル4aを参照してlabel「36」に応じたlabel「pop」を求め、labelをヌルにし(pop)、次のMPLSルータ5に向けて送信する。エッジルータ5はlabel=ヌルのフレームを受信すれば、MACフレームよりMPLSのshimヘッダを削除して宛先端末装置に向けて送信する。

【0014】MPLS用ルータであるLSR(label switching router)は、ルーティングテーブル情報などのIP層の経路情報を参照して経路を決定し、該経路にラベルを張る仕組みを有している。すなわち、LSRはIPのルーティングプロトコル(RIP,OSPFなど)が決めた経路に沿って、LDP(1a

bel distribution protocol)に従ってラベルパスを自動的に生成する。

【0015】図23はラベルパス設定の仕組みの説明図である。宛先端末装置側のエッジルータであるMPLSルータ(LSR)5はOSPF(open shortest path first)などのルーティングプロトコルを使って送信側MPLSルータ(LSR)1に向かう上流のルータ(LSP)4を求め、該ルータ(LSP)4に対しlabelをヌルにしてフレームを送出するよう依頼すると共に、宛先端末装置のIPアドレス(=10.1.100.0/24)を送る。これにより、MPLSルータ(LSR)4は空いているlabel値(=36)を求め、かつ、ルーティングプロトコルを使って送信側MPLSルータ(LSR)1に向かうMPLSルータLSP3を求め、該MPLSルータLSP4に対しlabelを「36」にしてフレームを送出するよう依頼すると共に、宛先端末装置のIPアドレス(=10.1.100.0/24)を送る。又、MPLSルータLSP4はラベルテーブル4aを作成する。このラベルテーブル4aは、①local label(=36)、② outgoing label(=pop label)、③ prefix (=10.1.100.0/24)、④MPLSルータ(LSR)5とのoutgoing interface(=ether 6)、⑤Next Hop(=MPLSルータ(LSR)5のIPアドレス)を含んでいる。以下、同様に、MPLS用ルータ(LSR)3、MPLS用ルータ(LSR)2はラベルテーブル3a, 2aを作成し、又、エッジルータであるMPLSルータ(LSR)1はラベルテーブル1aを作成する。

【0016】この状態において、宛先IPアドレス10.1.100.0/24のIPパケットを有するMACフレームが送信側端末よりエッジルータ1aに入力すると、図22で説明したようにMPLS用ヘッダを付加され、label fieldのlabel値をpush, swap, popしながらMPLS網を伝搬し、エッジルータ5aよりMPLS用ヘッダが削除されて宛先端末装置に送信される。

【0017】図24はMPLSのヘッダであるシムヘッダ(sim header)の構造とレイヤ2フレーム(MACフレーム)におけるシムヘッダの挿入位置説明図である。図中、M1はMAC宛先アドレス(MAC DA)、M2はMAC発信元アドレス(MAC SA)、M4はタイプ、M5はIPパケット(IPヘッダ/TCPヘッダ/データ部)である。M6はレイヤ2ヘッダとIPヘッダ間に挿入されるシムヘッダであり、20ビットのlabel field、3ビットのEXP field、1ビットのS field、8ビットのTTL fieldを有している。MPLSではシムヘッダのスタック(多重)が可能であり、スタックすることによりVPNを構築することができる。すなわち、図25(A)に示すように1つのIPパケットに2つのシムヘッダM6, M7を重ねて転送する。図25(B)に示すように、第1シムヘッダM6のlabel(階層1のlabel)はMPLSネットワーク内部の転送用として使用し、第2のlabel(階層2のlabel)はエッジルータ1, 5につながった回線のVPNを識別するため使用する。すなわち、第2のlabelはVPN識別用に使用される。又、ユーザ回線を識別するために第2のlabelを使用することもできる。

【0018】図26は2つのlabelをスタックしてIP-VPN

Nを実現するMPLS/VPNの説明図であり、エッジルータ1, 5を介してVPN Aのユーザが通信するものとする。予め、エッジルータ1, 5はユーザ回線インタフェース単位にVPN-ID(VPN識別子)を割り当てる。図では、エッジルータ1はVPN-Aサイトのネットワークアドレス=192.168.0.Xに対応してVPN-ID=13を割り当て、又、エッジルータ5はVPN-Bサイトのネットワークアドレス=192.168.1.Xに対応してVPN-ID=13を割り当て、VPN-Bサイトのネットワークアドレス=ZZZ.ZZZ.Z.Zに対応してVPN-ID=14を割り当てる。しかる後、受信側エッジルータ5はiBGP(inter border gateway protocol)に従って、VPN-ID/ネットワークアドレスの組み合わせ毎にlabel情報を送信側エッジルータ1に通知する。iBGPはTCPのコネクションを張って経路情報等をやり取りするプロトコルであり、このプロトコルに従ってMPLS網のエッジに位置するルータ同士がコアルータを素通りしてVPN情報の送受をする。図の例では、受信側エッジルータ5はiBGPを使って送信側エッジルータ1に、「192.168.1.X、VPN-ID=13」のラベルは「3」であると通知し、又、「ZZZ.ZZZ.Z.Z、VPN-ID=14」のラベルは「4」であると通知する。この情報を基にして、エッジルータ1はVPN-ID毎にラベルテーブル1a, 1bを作成する。

【0019】以上と並行して、各MPLS用ルータは図22、図23で説明したようLDP(label distribution protocol)によりパケットをMPLS網内部で転送するためのラベルパスを設定する。これにより、コアルータ2からエッジルータ1宛先192.168.1.XのMPLS転送用ラベルとして「5」が通知され、又、宛先ZZZ.ZZZ.Z.ZのMPLS転送用ラベルとして「5」が通知され、ラベルテーブル1a, 1bに追加される。以上のラベルテーブル1aが作成された状態において、VPN Aのユーザサイト(送信元VPN-ID=13)からIPパケットが入力すると、エッジルータ1は送信元VPN=13及び宛先IPアドレス=192.168.1.Xに基づいてテーブル1aを参照し、VPN判別用ラベル(=3)、MPLS転送用ラベル(=5)を求め、これら2つのラベルをパケットに付与してコアルータ2に送信する。コアルータ2はMPLS転送用ラベル(=5)を参照して転送処理を行い、受信側エッジルータ5はパケットが到達すると、VPN判別用ラベル(=3)を参照して該当VPNがVPN Aであると判断し、ラベルを取り除いてパケットをVPN Aのユーザサイトのみに送出する。尚、以上ではラベルテーブルを2つ設けた例であるが、実際はエッジルータに送信元VPN-IDの数だけテーブルが設けられ、各テーブルに送信元VPN-ID及び宛先IPアドレスの組み合わせに対応させてVPN判別用ラベルとMPLS転送用ラベルとが保持される。

【0020】図27はMPLS/VPNsの説明図であり、通信事業者(プロバイダ)のネットワークをMPLS網で構成した例である。11はプロバイダのMPLS網、12, 13, 14はMPLS網のエッジに位置するプロバイダエッジルータ(PEルータ)、15～18はMPLS網内に位置するコアルータ、21～24

は顧客システム(イントラネット)、25~28は顧客システムのエッジに位置する顧客エッジルータ(CEルータ)である。PEルータ12~15は2階層のMPLSをサポートし、かつ、VPNを意識するルータである。発信側PEルータはCEルータから入力するパケットに予めテーブルに設定されているVPN判別ラベル(VPN-ID)及びVPN判別用ラベルを付加し、又、受信側のPEルータは該パケットを受信すればそのVPN転送用ラベル(VPN-ID)に応じた顧客システムにパケットを送出する。図27の例では顧客システム21、22によりVPN Aが形成され、顧客システム23、24によりVPN Bが形成されている。従って、VPN-A内の各顧客システムの端末装置はVPN A内の端末装置にしかアクセスできず、VPN-Bの端末装置にアクセスすることはできない。同様に、VPN-B内の端末装置もVPN-B内の端末装置にしかアクセスできない。以上より、同一企業グループのみに同じVPN-IDを割り当てれば、他の企業グループからアクセスされることはなく、又、他の企業にデータが送信されることはなく、同一企業グループに閉じたIP-VPNを構築することができる。

【0021】

【発明が解決しようとする課題】VLANによるVPN構築方法によれば、ネットワーク上で各ユーザ毎にユニークなVIDを割り当てることで、容易に、かつ、安い設備投資でVPNを構成できる利点がある。しかし、VIDフィールドは最大12bitであり、10進数にすると、4,096個までしか設定することができない。この為、4,096個目以降のVIDを要求するユーザが現われた場合に対応できなくなり、小規模から大規模の幅広いネットワークの要請に対応できず、拡張性(スケーラビリティ)が低い問題がある。一方、MPLSによるVPN構築法によれば、VPN識別子を表現するlabel領域は20ビットであるため、VLANによる構築法に比べてはるかに多くのVPNを設定でき、インターネットの拡大に対応でき、拡張性が優れている利点がある。しかし、MPLSによるVPN構築法では、ユーザの近くまで高価なMPLS対応のルータを設置しなくてはならず、しかも、エッジルータの1ポートがユーザのために準備する必要があるなど非常に設備投資がかかる問題がある。

【0022】以上より、本発明の目的は、ネットワークにおいて、VLAN対応SwitchingHUBでアクセス系ネットワークを構築し、MPLS対応ルータでコアネットワークを構築するようにして安価な値段で且つスケール性の高いVPNを提供することである。又、本発明の別の目的は、VLANとMPLS間にインタフェースを設けることによりVLANとMPLSが共存できるようにし、かつ、VLANからMPLSへの移行を容易に行えるようにして、安価な値段で且つスケール性(拡張性)の高いVPNを提供することである。本発明の別の目的は、地域毎のアクセス系にVLAN対応スイッチングハブを使用し、地域間のWAN上にMPLSによるVPNを構築することで安価な値段で且つスケール性(拡張性)の

高いVPNを提供することである。本発明の別の目的は、VPNを構成する際に、IP以外のIPX, FNA, Apple Talk...等のプロトコルもユーザが利用可能な環境を提供することである。

【0023】

【課題を解決するための手段】上記課題は本発明の第1によれば、共有ネットワーク上にVPNを形成し、該VPNを介して通信を行うネットワークにおいて、ラベルスイッチ網でVPNのコア網を形成すると共に、VLANで該コア網に対するアクセス網を形成し、ラベルスイッチ網とVLAN間のインタフェース機能を実行する装置をこれらラベルスイッチ網の端に設けることにより達成される。このネットワークにおいて、インタフェース装置はMPLS網の端に設けられたエッジルータにより構成でき、送信側のエッジルータはVLANから送出されるパケットをMPLSのパケットに変換してラベルスイッチ網であるMPLS網に送出し、受信側のエッジルータはMPLS網より受信したMPLSのパケットをVLANのパケットに変換し、該VLANパケットを送信側VLANと同一のVPNに属するVLANに向けて送信する。

【0024】エッジルータは具体的には、VLANのパケットに含まれるVLAN識別子(VID)とMPLSのパケットに含まれるVPN識別子(VPNラベル)の対応を記憶するテーブルを備え、送信側エッジルータはVLANパケットのVIDに応じたVPNラベルを求め、該VPNラベルを有するMPLSパケットを生成してMPLS網に送出し、受信側エッジルータはMPLS網より受信したMPLSパケットに含まれるVPNラベルに応じたVIDを求め、該VIDを有するVLANパケットを生成し、該VIDが示すVLANに送出する。又、エッジルータは、受信側のエッジルータに向けてMPLSパケットを送出する経路を決定するルート決定部、ルート決定部により決定された経路を特定する転送用ラベルを受信側エッジルータのアドレスに対応させて記憶するラベルテーブルを備え、送信側エッジルータは、パケットの宛先MACに応じた受信エッジルータを求め、該ラベルテーブルより受信エッジルータに応じた転送用ラベルを求め、前記VPNラベル及び転送用ラベルを含むMPLSパケットを生成してMPLS網に送出する。

【0025】又、上記課題は本発明の第2によれば、共有ネットワーク上にVPNを形成し、MPLS網で該VPNのコア網を形成し、VLANで該コア網に対するアクセス網を形成するネットワークにおけるエッジルータにおいて、(1) VLAN識別子(VID)とVPN識別子であるVPNラベルの対応を記憶する手段、(2) 前記対応関係を用いてVLANから送出されるパケットに含まれるVIDに応じたVPNラベルを求め、該VPNラベルを含むMPLSパケットを生成してMPLS網に送出するMPLSパケット生成部を備えた送信側エッジルータにより達成される。このエッジルータは更に、(3) 受信側のエッジルータに向けてMPLSパケットを送出する経路を決定するルート決定部、(4) ルート決定部により

決定された経路を特定する転送用ラベルを受信側エッジルータに対応させて記憶する転送用ラベル記憶部を備え、(5) 前記MPLSパケット生成部は、パケットの宛先MACアドレスに応じた受信エッジルータを求め、ラベル記憶部より該受信エッジルータに応じた転送用ラベルを求め、前記VPNラベル及び転送用ラベルを含むMPLSパケットを生成する。

【0026】又、上記課題は本発明の第3によれば、共有ネットワーク上にVPNを形成し、MPLS網で該VPNのコア網を形成し、VLANで該コア網に対するアクセス網を形成するネットワークにおけるエッジルータにおいて、(1) VLAN識別子(VID)とVPN識別子であるVPNラベルの対応を記憶するテーブル、(2) 前記テーブルを用いてMPLS網より入力するパケットに含まれるVPNラベルに応じたVIDを求め、該VIDを含むVLANパケットを生成してMPLS網に送出するVLANパケット生成部、を備えた受信側のエッジルータにより達成される。

【0027】又、上記課題は本発明の第4によれば、共有ネットワーク上にVPNを形成し、MPLS網で該VPNのコア網を形成し、VLANで該コア網に対するアクセス網を形成するネットワークにおけるエッジルータにおいて、(1) VLAN識別子(VID)とVPN識別子であるVPNラベルの対応を記憶するテーブル、(2) 前記テーブルを用いてVLANより入力するパケットに含まれるVIDに応じたVPNラベルを求め、該VPNラベルを含むMPLSパケットを生成してMPLS網に送出するMPLSパケット生成部、(3) 前記テーブルを用いてMPLS網より入力するパケットに含まれるVPNラベルに応じたVIDを求め、該VIDを含むVLANパケットを生成してMPLS網に送出するVLANパケット生成部、を備えたエッジルータにより達成される。

【0028】

【発明の実施の形態】(A) 本発明の概略

図1は本発明のVLANとMPLS混在ネットワークの概略図であり、101～104は拠点A～DのVLANであり所定のVID(VLAN ID)で管理されている。110はインターネット(WAN)上にMPLSにより構築されたlabelで管理される共有ネットワーク(MPLSネットワーク)、111～114はMPLS網のエッジ部に設けられたエッジルータである。送信側のエッジルータ111～114はVLAN101～104から入力するVLANパケット(図20)をMPLSパケット(図25(A))に変換して送信し、受信側のエッジルータはMPLSパケットをVLANパケットに変換して所定のVLANに出力する。

【0029】すなわち、送信側エッジルータは、VLANパケットに含まれるVIDをVPN識別子であるVPNラベルに変換すると共に、VLANパケットの宛先に基づいて該パケットを所定の経路に沿って転送するための転送用ラベルを求め、VIDに替えてこれらラベルを付加してMPLSパケットを生成してMPLS網110に送出する。MPLS網110は予め設定されているルートにそって転送用ラベルを付け替えながらMPLSパケットを目的の受信側エッジルータまでルー

チングする。受信側エッジルータはMPLS網よりMPLSパケットを受信すれば、転送用ラベルを削除すると共に、VPNラベルを元のVIDに変換し、ラベルに替えて該VIDを付加してVLANパケットを生成し、該VLANパケットをVIDが示すVLANに送出する。以上、所定のVPNに属する送信側VLANから同一のVPNに属する受信側VLANにパケットを送信することができる。

【0030】図2はエッジルータ111の概略構成図であり、他のエッジルータも同一の構成を備えている。エッジルータ111のラインカード部121はEthernetインタフェースの機能を備え、所定のVLANよりVLANパケットを受信する。VPN識別部122は受信したVLANパケットのVIDを参照してVPNを識別し、該VPNに応じたタグ/ラベル交換部(サブルータ)123i(i=1,2,...)へ入力する。識別されたVPNに応じたサブルータ123iのテーブル124には例えば図4に示すように、①VLAN ID(VID)と、②該VIDにより特定されるVLANが所属するVPNを特定するVPN識別子(VPNラベル)の対応が予め記憶されている。又、ルート決定部131は、ルーチングプロトコル132を用いて受信側エッジルータへの経路を予め決定し、MPLS網ルーチングテーブル(転送用ラベル記憶部)133に受信側エッジルータのIPアドレスに対応させて前記決定した経路を特定する転送用ラベル(pushラベル)を記憶する。

【0031】サブルータ123iは、パケットが入力すると、タグに含まれるVIDに応じたVPN識別子(VPNラベル)をテーブル124より求める。又、サブルータ123iはパケットに含まれる宛先アドレスに基づいて受信側エッジルータを求め、該エッジルータのIPアドレスに対応させて記憶されている転送用ラベルをMPLS網ルーチングテーブル133より求める。ラベルが求めれば、サブルータ123iはパケットのタグに替えてVPNラベル及び転送用ラベルを挿入し(swap)、ラインカード部128を介してMPLS網111に送出する。以後、MPLS網110は予め設定されている経路にそって転送用ラベルを付け替えながらMPLSパケットを目的の受信側エッジルータまでルーチングする。受信側エッジルータのラインカード部128はMPLS網110よりMPLSパケットを受信し、VPN識別部129はMPLSのVPNラベルを参照してVPNを識別し、該VPNに応じたサブルータ123i(i=1,2,...)へ入力する。

【0032】サブルータ123iは転送用ラベルを削除すると共に、テーブル124を参照してVPNラベルに応じたVIDを求める。ついで、VPNラベルに替えて求めたVIDを含むタグを付加してVLANパケットを生成し、該VLANパケットをVLAN側のラインカード部121を介してVIDが示すVLANに送出する。尚、各エッジルータ111～114におけるテーブル124の内容は同一でなく、同一のVPNに属するVLANのVID値は同じとは限らない。また、図2では明確に示さなかったが、サブルータは図5に示すようにVPN毎に存在する。以上より、図1において拠点AのVLAN 101から拠点DのVLAN 104に通信が発生すると、図3に示すよう

にタグとラベルのスイッチがエッジルータ111,114で行なわれる。これにより送信側VLANより入力するVLANパケットはエッジルータ111でMPLSパケットとなってMPLS網を伝送し、エッジルータ114でVLANパケットに変換され、送信側VLANと同一のVPNに属するVLANに送信される。

【0033】(B) MPLSによる企業のネットワーク形態
図6はMPLS網を用いた企業のネットワーク形態説明図であり、200は共有ネットワークであるインターネット上に形成されたMPLS網、201はVLAN Domain 東京、202はVLAN Domain 名古屋、203はVLAN Domain 大阪、204はインターネット、205はファイアウォール(FW)であり、各VLAN Domain には複数の企業のVLANが構成されている。MPLS網200と各VLAN Domain 201~203間であって、MPLS網のエッジにはVLANを終端するプロバイダエッジルータ(Provider Edge Router:PE) 211~213が設けられている。

【0034】VLAN Domain 東京201には東京地区のA企業のVLAN(VID=101)、B企業のVLAN(VID=2)が形成されている。A企業のVLAN(VID=101)を構成するCPEルータ(Customer Premise Equipment Edge Router) 212は、EthernetによりL2Switch(スイッチングハブ) 213を介してエッジルータPE 211の第1のポートに接続している。又、B企業のVLAN(VID=2)を構成するCPEルータ214は、Ethernetを介してL2Switch(スイッチングハブ) 215に接続され、該スイッチングハブ215はエッジルータPE 211の第2のポートに接続されている。VLAN Domain 名古屋202には名古屋地区のA企業のVLAN(VID=152)、C企業のイントラネットが形成されている。A企業のVLAN(VID=152)を構成するCPEルータ221は、EthernetによりL2Switch(スイッチングハブ) 222を介してエッジルータPE 212の第1のポートに接続している。又、C企業のイントラネット223のCPEルータ224は、エッジルータPE 212の第2のポートに接続されている。VLAN Domain 大阪203には大阪地区のA企業のVLAN(VID=1501)、C企業のイントラネットが形成されている。A企業のVLAN(VID=1501)を構成するCPEルータ231は、EthernetによりL2Switch(スイッチングハブ) 232を介してエッジルータPE 213の第1のポートに接続している。又、C企業のイントラネット233のCPEルータ234は、エッジルータPE 213の第2のポートに接続されている。

【0035】各地区におけるA企業のVLAN(VID=101)、VLAN(VID=152)、VLAN(VID=1501)は同一のVPNを構成している。従って、A企業側からMPLS網側を見ると、図7(A)に示すように各CPEルータ212, 221, 231がレイヤ2のスイッチングハブSHBに接続されているように見え、A企業のネットワークはコア網をMPLS網で構成し、アクセス網をVLANで構成してなるL2(VLAN) over MPLSネットワーク形態となる。又、B企業からMPLS網側を見ると、図7(B)に示すようにCPEルータ214及びファイアウォール205がレイヤ2/3のスイッチングハブSHB'に接

続されているように見え、B企業のネットワークはインターネット接続形態となる。又、C企業からMPLS網側を見ると、図7(C)に示すようにイントラネット223, 233のCPEルータ224, 234がルータRTに接続されているように見え、C企業のネットワークはMPLSでVPNを構成したMPLS/VPNsネットワーク形態となる。

【0036】(C) L2(VLAN) over MPLSネットワーク
図8は図6よりA企業に関連する部分を書き出した本発明のL2(VLAN) over MPLSネットワークの全体図であり、図6と同一部分には同一符号を付し、VLANを構成するルータCPEA 212, 221, 231にはL2アドレスであるMACアドレスMAC A, MAC B, MAC Cが付されている。

【0037】(D) エッジルータの構成
各エッジルータPEA~PECは同一の構成を備えている。図9はエッジルータの構成図であり、図2に示したエッジルータを詳細に示すもので、図2のエッジルータと同一部分には同一符号を付している。ラインカード部121はEthernetインタフェースの機能を備え、所定のVLANよりVLANパケットを受信する。VPN識別部122は受信したVLANパケットのVIDを参照してVPNを識別し、VPNに応じたサブルータ123i(i=1,2,...)へパケットを入力する。サブルータ123iのVPNラベルテーブル124には図10に示すように、①VPNラベル(VPN識別子)、②配下であるCPEルータのL2アドレス(MACアドレス)、③出力側インタフェース、④エッジルータに接続するVLANの識別子(VID)、⑤VPNi(VPNinstance:VPN識別子の便宜名)の対応が予め記憶されている。

【0038】又、L2VPNルーティングテーブル125には、図10に示すようにVPNを構成するVLAN毎に、①該VLAN内のCPEルータのL2アドレス(MACアドレス)、②CPEルータが接続するエッジルータのループバックアドレス(IPアドレス)、③CPEルータの属するVLANの識別子(VID)を保持する。図8の例では、VLAN(VID=101)、VLAN(VID=152)、VLAN(VID=1501)のそれぞれに対応させて、①CPEルータ212, 221, 231のMACアドレスMAC A, MAC B, MAC C、②各CPEルータが接続するエッジルータ(PEA, PEB, PEC) 211, 212, 213のループバックアドレス(IPアドレス)、③各CPEルータの属するVLANのVID(=101, 152, 1501)が保持されている。

【0039】MPLS網ルーティングテーブル(転送用ラベルテーブル)133は受信エッジルータへの経路を特定する通信用ラベルを記憶する。同一VPNに属するVLAN間で通信できるように、予めMPLS網内のルータのルート決定部はルーティングプロトコルを用いて送信側エッジルータから受信側エッジルータに至る経路を探索し、LDP(Label Distribution Protocol)に従って各経路にLabelを割り当てる。従って、送信側エッジルータのルート決定部11は、ルーティングプロトコル132を用いて受信側エッジルータへの経路を決定し、転送用ラベルテーブル133に受信側エッジルータのループバック(IPアドレス)に対応さ

せて前記決定した経路を特定する転送用ラベル(pushラベル)を記憶する。

【0040】サブルータ123iのVPNラベル処理部126は、VLANパケット(図20参照)が入力すると、タグに含まれるVIDに応じたVPN識別子(VPNラベル)をVPNラベルテーブル124より求める。又、ルーチングテーブル処理部127はVLANパケットに含まれる宛先MACアドレスに基づいてL2VPNルーチングテーブル125より出力側エッジルータのループバックアドレスを求め、ついで、転送用ラベルテーブル133より該ループバックアドレス(IPアドレス)に対応する転送用ラベル(pushラベル)を求める。VPNラベル、pushラベルが求めれば、サブルータ123iは図3に示すようにタグに替えてVPNラベル及び転送用ラベルを挿入してMPLSパケットを生成し(swap)、該MPLSパケットをラインカード部128を介してMPLS網に送出する。

【0041】以後、予め設定されているMPLS網内の経路にそって転送用ラベルを付け替えながらMPLSパケットが目的の受信側エッジルータに到達する。受信側エッジルータのラインカード部128はMPLS網110よりMPLSパケットを受信し、VPN識別部129はMPLSのVPNラベルを参照してVPNを識別し、該VPNに応じたサブルータ123i(i=1,2,...)へ入力する。サブルータ123iは転送用ラベルを削除する共に、VPNラベルテーブル124を参照してVPNラベルに応じたVIDを求める。ついで、VPNラベルに替えて求めたVIDを含むタグを付加してVLANパケットを生成し(swap)、該VLANパケットをラインカード部121を介してVIDが示すVLANに送出する。尚、各エッジルータ211~213(図8)におけるVPNラベルテーブル124の内容は同一でなく、同一のVPNに属するVLANのVID値は同じとは限らない。また、図9では明確に示さなかったが、サブルータ123i(i=1,2,...)や転送用ラベルテーブル133はVPN毎に存在する。

【0042】(E) VPNテーブルの生成

VPNに属するVLAN同士で通信を行えるようにするには、(1) 予めこれらVLANが接続するエッジルータ間のルートを設定し、該ルートに沿ったルータの転送用ラベルテーブル133(図9)に転送用ラベルを記憶し、かつ、(2) VPNラベルテーブル124、L2VPNルーチングテーブル125を作成する必要がある。(1)の転送用ラベルテーブル133の作成方法は周知であるため説明はしない。VPNラベルテーブル124、L2VPNルーチングテーブル125を作成するには、図10(A)に示すように、まず、VPNの識別子(VPNラベル)、VLAN識別子(VID)、VPNiをオペレータが手入力する。これらデータがエッジルータに入力されると、該エッジルータのVPNラベル処理部126は、自分に接続するVLANのCPEルータのMACアドレスをARP(Address Resolution Protocol)を使って求め、又、pushラベルが付されたMPLSパケットを送出する経路のインタフェースを求め、図10(B)に示すように設定してVPNラベルテーブル124を作成する。

【0043】ついで、ルーチングテーブル処理部127

は、自エッジルータに接続するCPEルータのMACアドレス及びVLAN識別子(VID)をVPNラベルテーブル124より求めてL2VPNルーチングテーブル125のdirectConnect情報を作成する(図10(B)参照)。しかる後、VPNを構成する各VLAN(VID=101, 152, 1501)と接続するエッジルータ(PEA, PEB, PEC)211, 212, 213はそれぞれiBGPを用いて、自エッジルータに接続するユーザルータCPEのMACアドレスと自エッジルータのループバックアドレス(IPアドレス)、VIDを組にして他のエッジルータに送出する。これにより、各エッジルータは受信情報に基づいてL2VPNルーチングテーブル125を完成する(図10(B)参照)。以上により、各エッジルータ211, 212, 213のそれぞれには図8のA企業のVPNについて図11(A)~(C)に示すVPNテーブルが作成される。

【0044】(F) CPEAからCPECへの通信例

図12は東京のA企業のVLAN(VID=101)に属するユーザルータCPEAから大阪のA企業のVLAN(VID=1501)に属するユーザルータCPECにパケットを送信する送信例である。ユーザルータCPEAはVID=101を有するタグが付加されたVLANパケットPKT1を送出する。エッジルータPEA 211はパケットPKT1が入力するとタグを外し、代わりにVPNラベル(=26:企業AのVPN識別子)と転送用ラベル(=pushラベル)を付加してなるMPLSパケットPKT2を生成してMPLS網200に送出する。以後、MPLSパケットPKT2は予め設定されているMPLS網内の経路にそって転送用ラベルを付け替えながら目的の受信側エッジルータPEC 213に到達する。受信側エッジルータPEC 213はラベルを外し、宛先のユーザルータCPECが属するVLAN識別子(VID=1501)を付加してVLANパケットPKT3を作成し、VID=1501が指示するVLANに送出する。これにより、VLANパケットPKT3はユーザルータ231に到達する。

【0045】(G) L2(VLAN) over MPLSの送信処理

図13及び図14はL2(VLAN) over MPLSの送信処理フローである。送信側エッジルータはパケットが入力すると該パケットにタグが付加されているかチェックし(ステップ301)、付加されていないければMPLSパケットであるから通常のMPLSの処理を行い、タグが付加されていれば、該タグに含まれるVLAN ID(=VID)の値を抽出し(ステップ302)、VID値が4096以上であるかチェックする(ステップ303)。4096以上であれば、VID値の範囲0~4095を越えているため該パケットを破棄する。しかし、VID値が0~4095の範囲に入っていれば、VLAN IDとVPNラベルの変換テーブル124を参照し(ステップ304)、VPNラベル値が発見されたかチェックする(ステップ305)。発見されなければ通常のMPLS対応の処理を行い、発見されれば、タグを外して2層目のラベル値(VPNラベル)をつける(ステップ306)。

【0046】しかる後、パケットの宛先MACアドレスより受信側エッジルータのループバックアドレス(IPアド

レス)をL2VPNルーティングテーブル125より求める(ステップ307)。ループバックアドレスが求めれば、転送用ラベルテーブル133を参照して転送用ラベル(pushラベル)を求め(ステップ308)、該pushラベルを1階層目につけてMPLS網に送出する(ステップ309)。以上は送信側エッジルータの処理である。以後、MPLS網内でのラベルルーティング処理が行われ、MPLSパケットは予め設定されているMPLS網内の経路にそって転送用ラベルを付け替えながら目的の受信側エッジルータに向けて転送される(ステップ310)。

【0047】受信側エッジルータはMPLSパケットが到着したかチェックし(ステップ311)、到着すれば、1階層目に付属されている転送用ラベルを削除する(ステップ312)。ついで、2階層目のVPNラベルを抽出し(ステップ313)、VLAN ID(=VID)とVPNラベルとの対応テーブル124を参照し(ステップ314)、VIDが発見されたかチェックする(ステップ315)。VIDが発見されなければパケットを破棄し、VIDが発見されれば、2階層目のラベルを外し、該VIDを含むタグをつけてVLANパケットを作成する(ステップ316)。ついで、VPNラベルテーブル124を参照して出力インタフェースを求め、該インタフェースにVLANパケットを送出し(ステップ317)、宛先のユーザルータCPECはVLANパケットを受信して所定の処理を行う(ステップ318)。

【0048】(H) VPNテーブルの更新処理
VPNの構成は企業ポリシーにより拡大、変更が行われて刻々と変化する。そこで、VPNの構成変化に応じてVPNテーブル124、125を更新する必要がある。図15はユーザルータCPEAがユーザルータCPECと通信する場合の更新説明図である。

1. ユーザルータCPEA 212は宛先のユーザルータCPECのMACアドレスが不明であれば、ルータCPECのIPアドレスを含むARPパケットをブロードキャストする。
2. エッジルータPEA 211は該ARPパケット(ブロードキャストパケット)を受信すれば、該パケットのコピーを作成し、他のエッジルータPEB、PEC 212, 213に流す。
3. ユーザルータCPECは自分のIPアドレスを含むARPパケットを受信すれば、ARP-replyパケットに自分のMACアドレスを乗せて返送する。各エッジルータPEはARP-replyパケットによりVPNラベルテーブル124, VPNルーティング125における各CPEのMACアドレスを自動的に更新する。
4. 又、定期的に、各ルータのIPアドレスを含むARPパケットをブロードキャストして各テーブルを更新する。

【0049】(I) 同一VPNに属するVLAN同士の通信を禁止する処理

図10、図11を参照して説明したVPNテーブルの作成処理では、VLAN同士が自由に通信を行える場合であったが、同じVPNに属していても所定VLAN同士の通信を禁止したい場合がある。かかる場合、通信禁止のVLANが属するエッジルータ間においてiBGPによるルーティング情報の

通信を停止する。このようにすれば、L2VPNルーティングテーブル125に通信禁止先ルータCPEのMACアドレス、該ルータCPEが接続するエッジルータのループバックアドレス(IPアドレス)が登録されなくなり、通信を行うことができなくなる。

【0050】図16は通信禁止のVLANが存在する場合のL2VPNルーティングテーブル125の作成処理フローである。所定VPNについて、各エッジルータPEにVLAN ID(VID)及びVPN識別子(VPNラベル)を設定入力する(ステップ401)。ついで、通信禁止VLANのペアを入力する(ステップ402)。各エッジルータPEはVPNラベルテーブルを自動作成し(ステップ403)、ついで、各エッジルータPEはL2VPNルーティングテーブル125のdirectConnect 情報を作成する(ステップ404)。

【0051】しかる後、iBGPを使って、VPNルーティング情報(ユーザルータCPEのMACアドレス、エッジルータのループバックアドレス等)を通信禁止されていないVLANが配下となっているエッジルータPEに送信する(ステップ405)。しかし、通信禁止されているVLANが配下となっているエッジルータPEにはVPNルーティング情報を送信しない。各エッジルータPEは他のエッジルータから送られてくるルーティング情報を受信し、該ルーティング情報を用いてL2VPNルーティングテーブル125を作成する(406)。以上により、エッジルータPEのL2VPNルーティングテーブル125には通信禁止先ルータCPEのMACアドレス、該ルータCPEが接続するエッジルータアドレスが登録されない。この結果、転送用ラベルを取得することができず通信禁止先のVLANとは通信を行うことができなくなる。

【0052】(J) VLANのuser priority とMPLSにおけるIP Precedence

図17(A)に示すようにVLANパケットのタグは3ビットのuser priorityを含み、この3ビットで各MACで規定されたプライオリティを入れるようになっている。プライオリティ値は0～7の8レベルがあり、数値が小さければ(例えば0)、ユーザプライオリティが低く、数値が大きければプライオリティが高い。一方、図18(B)に示すようにMPLSパケットのラベルは3ビットの実験用フィールドEXPを含み、この3ビットを用いてIP Precedenceを表現する。このIP Precedenceもプライオリティ値は0～7の8レベルがあり、数値が小さければ(例えば0)、プライオリティが低く、数値が大きければプライオリティが高い。そこで、エッジルータでVLANパケットからMPLSパケットに変換する際、3ビットのuser priorityをEXPフィールドに挿入し、又、MPLSパケットからVLANパケットに変換する際、3ビットのEXP フィールドのIP Precedenceをuser priority フィールドに挿入する。このようにすれば、VLANにおける優先制御をMPLS網におけるIP Precedence制御として継続でき、又、IP Precedence制御から元のVLANにおける優先制御に戻すことができる。

【 0 0 5 3 】・付記

(付記 1) 共有ネットワーク上にVPNを形成し、該VPNを介して通信を行うネットワークにおいて、ラベルスイッチ網でVPNのコア網を形成すると共に、VLANで該コア網に対するアクセス網を形成し、ラベルスイッチ網とVLAN間のインタフェース機能を実行する装置をこれらラベルスイッチ網の端に設けた、ことを特徴とするネットワーク。

【 0 0 5 4 】(付記 2) 前記インタフェース装置は、ラベルスイッチ網であるMPLS網の端に設けられたエッジルータであり、送信側のエッジルータはVLANから送出されるパケットをMPLSのパケットに変換してMPLS網に送出し、受信側のエッジルータはMPLS網より受信したMPLSのパケットをVLANのパケットに変換し、該VLANパケットを送信側VLANと同一のVPNに属するVLANに向けて送信する、ことを特徴とする付記 1 記載のネットワーク。

【 0 0 5 5 】(付記 3) 前記エッジルータはVLANのパケットに含まれるVLAN識別子(VID)とMPLSのパケットに含まれるVPNラベルの対応を記憶するテーブルを備え、送信側エッジルータはVLANパケットのVIDに応じたVPNラベルを求め、該VPNラベルを有するMPLSパケットを生成してMPLS網に送出し、受信側エッジルータはMPLS網より受信したMPLSパケットに含まれるVPNラベルに応じたVIDを求め、該VIDを有するVLANパケットを生成し、該VIDが示すVLANに送出する、ことを特徴とする付記 2 記載のネットワーク。

【 0 0 5 6 】(付記 4) 前記エッジルータは、受信側のエッジルータに向けてMPLSパケットを送出する経路を決定するルート決定部、ルート決定部により決定された経路を特定する転送用ラベルを受信側エッジルータのアドレスに対応させて記憶するテーブルを備え、送信側エッジルータは、パケットの宛先MACアドレスに応じた受信エッジルータを求め、該テーブルより受信エッジルータに応じた転送用ラベルを求め、前記VPNラベル及び転送用ラベルを含むMPLSパケットを生成してMPLS網に送出する、ことを特徴とする付記 3 記載のネットワーク。

【 0 0 5 7 】(付記 5) 前記VPNを構成するVLANに接続するエッジルータはそれぞれ、該エッジルータに接続するVLAN構成装置のアドレスとエッジルータのアドレスを組にして前記他のエッジルータに送出し、各エッジルータは受信情報に基づいてレイヤ2ルーティングテーブルを作成し、送信側エッジルータは、該レイヤ2ルーティングテーブルより前記パケットの宛先に応じた受信エッジルータを求める、ことを特徴とする付記 4 記載のネットワーク。

【 0 0 5 8 】(付記 6) エッジルータは通信が禁止されているVLANが接続されたエッジルータに上記のアドレス情報を送信しない、ことを特徴とする付記 5 記載のネットワーク。

(付記 7) 送信側エッジルータは、VID値が設定値以上

のVLANパケットを廃棄することを特徴とする付記 2 記載のネットワーク。

(付記 8) 送信側エッジルータはVLANパケットのタグに含まれるユーザ優先情報をMPLS網のIP優先情報としてMPLSパケットのラベルに挿入し、受信側エッジルータはMPLSパケットのラベルに含まれるIP優先情報をVLANのユーザ優先情報としてVLANパケットのタグに挿入する、ことを特徴とする付記 2 記載のネットワーク。

【 0 0 5 9 】(付記 9) 共有ネットワーク上にVPNを形成し、MPLS網で該VPNのコア網を形成し、VLANで該コア網に対するアクセス網を形成するネットワークにおけるエッジルータにおいて、VLAN識別子(VID)とVPN識別子であるVPNラベルの対応を記憶する手段、前記対応関係を用いてVLANから送出されるパケットに含まれるVIDに応じたVPNラベルを求め、該VPNラベルを含むMPLSパケットを生成してMPLS網に送出するMPLSパケット生成部、を備えたことを特徴とする送信側エッジルータ。

【 0 0 6 0 】(付記 1 0) 前記エッジルータは更に、受信側のエッジルータに向けてMPLSパケットを送出する経路を決定するルート決定部、ルート決定部により決定された経路を特定する転送用ラベルを受信側エッジルータに対応させて記憶する転送用ラベル記憶部、を備え、前記MPLSパケット生成部は、パケットの宛先MACアドレスに応じた受信エッジルータを求め、該転送用ラベル記憶部より受信エッジルータに応じた転送用ラベルを求め、前記VPNラベル及び転送用ラベルを含むMPLSパケットを生成する、ことを特徴とする付記 9 記載のエッジルータ。

【 0 0 6 1 】(付記 1 1) 前記MPLSパケット生成部は、前記VPNを構成する他のVLANに接続するエッジルータより送られてくる該エッジルータのアドレスと該エッジルータに接続するVLAN構成装置のアドレスとの組み合わせ情報に基づいてレイヤ2ルーティングテーブルを作成し、該レイヤ2ルーティングテーブルよりパケットの宛先に応じた前記受信エッジルータを求める、ことを特徴とする付記 1 0 記載のエッジルータ。

【 0 0 6 2 】(付記 1 2) 共有ネットワーク上にVPNを形成し、MPLS網で該VPNのコア網を形成し、VLANで該コア網に対するアクセス網を形成するネットワークにおけるエッジルータにおいて、VLAN識別子(VID)とVPN識別子であるVPNラベルの対応を記憶するテーブル、前記テーブルを用いてMPLS網より入力するパケットに含まれるVPNラベルに応じたVIDを求め、該VIDを含むVLANパケットを生成してMPLS網に送出するVLANパケット生成部、を備えたことを特徴とする受信側のエッジルータ。

【 0 0 6 3 】(付記 1 3) 共有ネットワーク上にVPNを形成し、MPLS網で該VPNのコア網を形成し、VLANで該コア網に対するアクセス網を形成するネットワークにおけるエッジルータにおいて、VLAN識別子(VID)とVPN識別子であるVPNラベルの対応を記憶するテーブル、前記テ

ブルを用いてVLANより入力するパケットに含まれるVIDに応じたVPNラベルを求め、該VPNラベルを含むMPLSパケットを生成してMPLS網に送出するMPLSパケット生成部、前記テーブルを用いてMPLS網より入力するパケットに含まれるVPNラベルに応じたVIDを求め、該VIDを含むVLANパケットを生成してMPLS網に送出するVLANパケット生成部、を備えたことを特徴とするエッジルータ。

【0064】(付記14) エッジルータは更に、受信側のエッジルータに向けてMPLSパケットを送出する経路を決定するルート決定部、ルート決定部により決定された経路を特定する転送用ラベルを受信側エッジルータに対応させて記憶する転送用ラベル記憶部、を備え、前記MPLSパケット生成部は、パケットの宛先に応じた受信エッジルータを求め、該転送用ラベル記憶部より受信エッジルータに応じた転送用ラベルを求め、前記VPNラベル及び転送用ラベルを含むMPLSパケットを生成する、ことを特徴とする付記13記載のエッジルータ。

【0065】(付記15) 前記MPLSパケット生成部は、前記VPNを構成する他のVLANに接続するエッジルータより送られてくる該エッジルータのアドレスと該エッジルータに接続するVLAN構成装置のアドレスとの組み合わせ情報に基づいてルーティングテーブルを作成し、該ルーティングテーブルよりパケットの宛先に応じた前記受信エッジルータを求める、ことを特徴とする付記14記載のネットワーク。

【0066】

【発明の効果】以上本発明によれば、MPLSのVPN識別子(VPNラベル)を20ビットで表現でき、キャリアネットワークのコア部分においてこのMPLSを使用することにより、VLANによる構築法に比べてはるかに多くのVPNを設定でき、VLANによるVPN数の限界値4,096の問題をクリアでき、スケール性の高いVPNを提供できる。又、本発明によれば、VLAN対応SwitchingHUBでアクセス系ネットワークを構築し、MPLS対応ルータでコアネットワークを構築することにより、安価なVPN(L2(VLAN) over MPLS形態のネットワーク)を構築できる。すなわち、本発明によれば、高価なMPLS対応ルータを地域内に設置せず、地域毎のアクセス系にVLAN対応スイッチングハブを使用し、かつ、地域間のWAN上にMPLSによるVPNを構築することで安価な値段で且つスケール性(拡張性)の高いVPNを提供することができる。

【0067】又、本発明によれば、VLANとMPLS間にパケット変換を行うインタフェース(エッジルータ)を設けたから、VLANとMPLSのネットワークを共存させたり、VLANからMPLSの移行を容易に行うことができ、安価な値段で且つスケール性の高いVPNを提供することができる。

又、本発明によれば、VLANとMPLSの統合するネットワー

ク手法、技術、製品を提供できるようにしたから、VLANで組まれた既存ネットワークを容易にL2(VLAN) over MPLSに移行することが出来る。

【図面の簡単な説明】

【図1】本発明のVLANとMPLSの混在ネットワークの概略図である。

【図2】エッジルータの概略構成図である。

【図3】VLANとMPLSのパケットの交換説明図である。

【図4】VIDとVPNラベルの変換テーブルである。

【図5】エッジルータの別の構成図である。

【図6】MPLS利用による企業のネットワーク形態説明図である。

【図7】企業のネットワーク形態説明図である。

【図8】L2 over MPLSネットワークである。

【図9】PEルータ(エッジルータ)の内部構造である。

【図10】VPNテーブルの生成説明図である。

【図11】各エッジルータにおける企業のVPNテーブル説明図である。

【図12】CPEAからCPECへの送信説明図である。

【図13】L2(VLAN) over MPLSの送信処理フロー(その1)である。

【図14】L2(VLAN) over MPLSの送信処理フロー(その2)である。

【図15】CPEAからCPECへ通信する場合における学習説明図である。

【図16】通信禁止VLANが存在する場合におけるL2VPNテーブル作成処理フローである。

【図17】VLANにおけるユーザプライオリティとMPLSにおけるIP Precedenceの対応説明図である。

【図18】ポートベースVLANの構成例である。

【図19】複数のスイッチングハブに属するポートをグループ化したVLAN構成例である。

【図20】VLANのMACフレームフォーマットである。

【図21】VLANの実現例である。

【図22】MPLS説明図である。

【図23】ラベル設定の仕組み説明図である。

【図24】シムヘッダの構造及び挿入位置説明図である。

【図25】シムヘッダのスタック説明図である。

【図26】MPLS/VPNの説明図である。

【図27】MPLS/VPNsの説明図である。

【符号の説明】

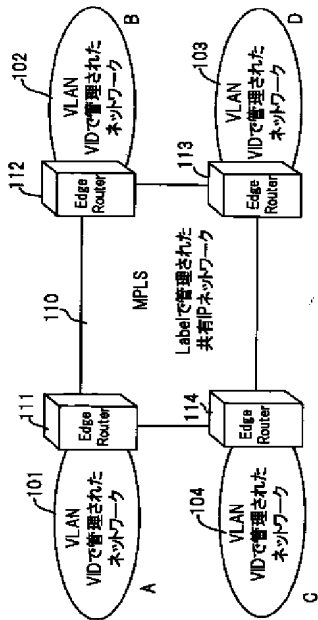
101～104・・・拠点A～DのVLAN

110・・・MPLSネットワーク

111～114・・・MPLS網のエッジ部に設けられたエッジルータ

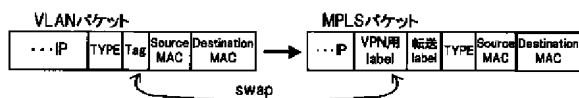
【図1】

本発明のVLANとMPLSの混在ネットワークの概略図



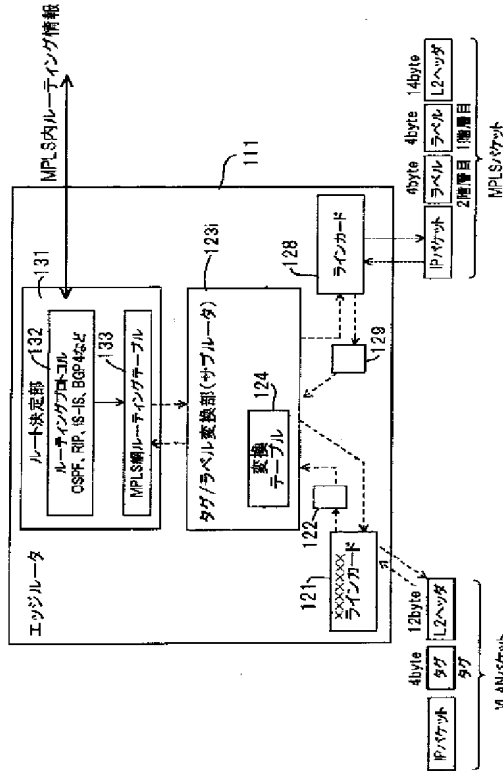
【図3】

VLANとMPLSのパケットの交換説明図



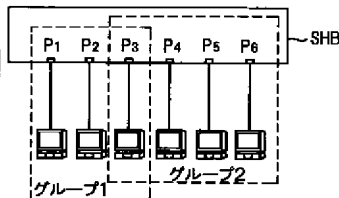
【図2】

エッジルータの概略構成



【図18】

ポートベース VLANの構成例



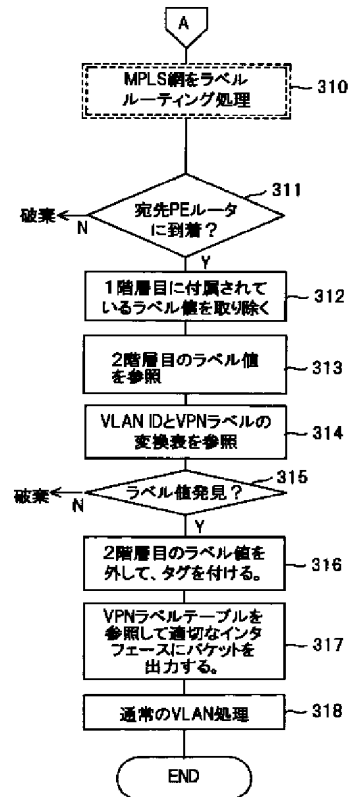
【図4】

VIDとLabelの交換テーブル

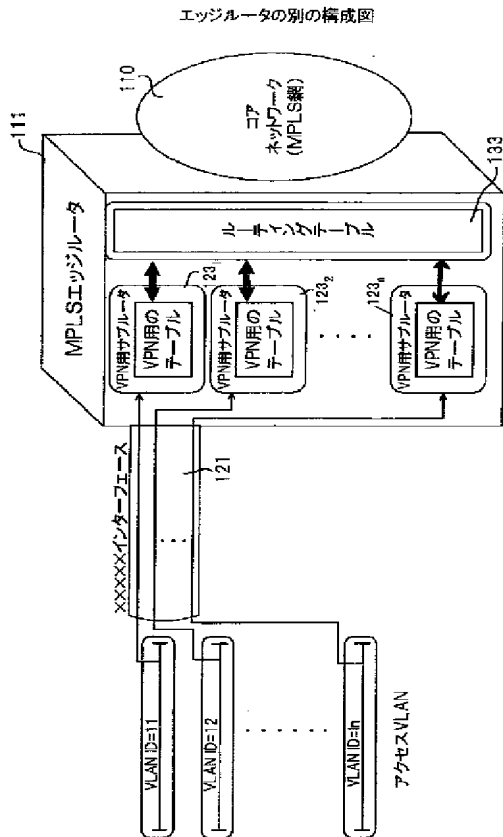
VLAN ID(VID)	VPN ラベル
N	M
N+1	M+1
.	.
.	.
N'	M'

【図14】

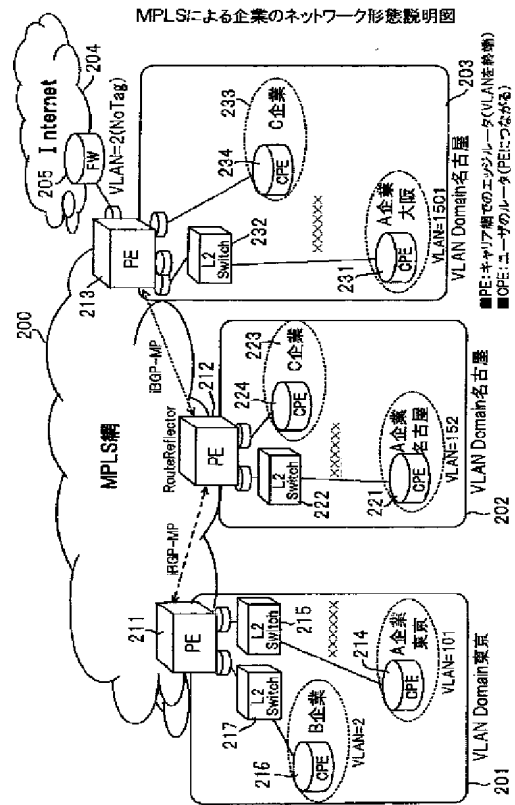
L2(VLAN) over MPLSの送信処理(その2)



【図5】

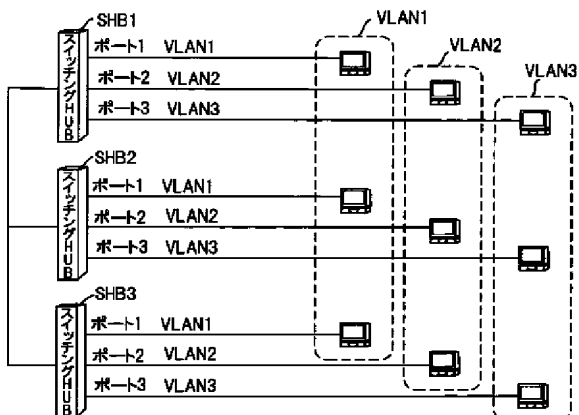


【図6】



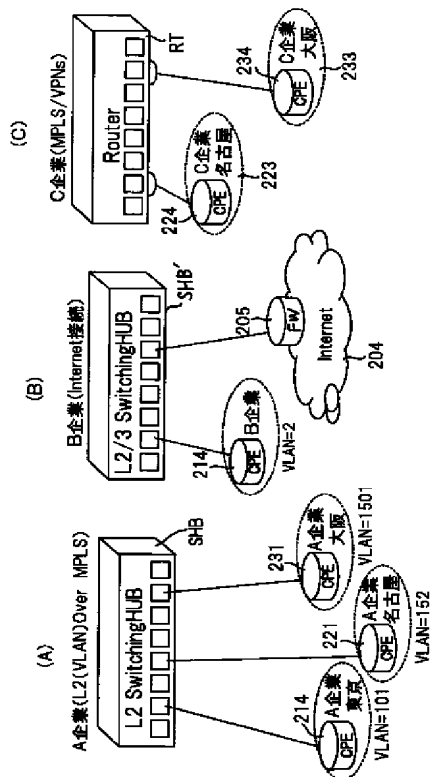
【図19】

複数のスイッチングハブに属するポートをグループ化したVLAN構成例



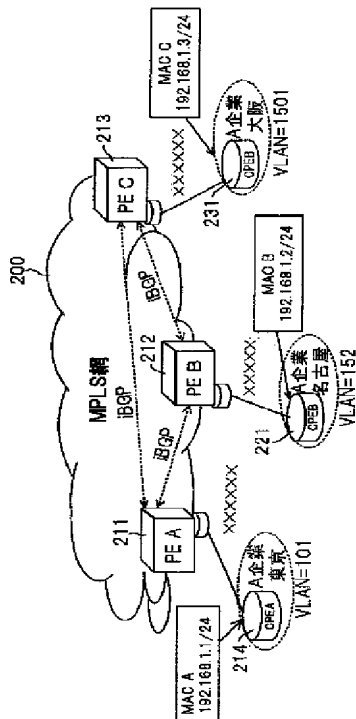
【図7】

企業のネットワーク形態説明図

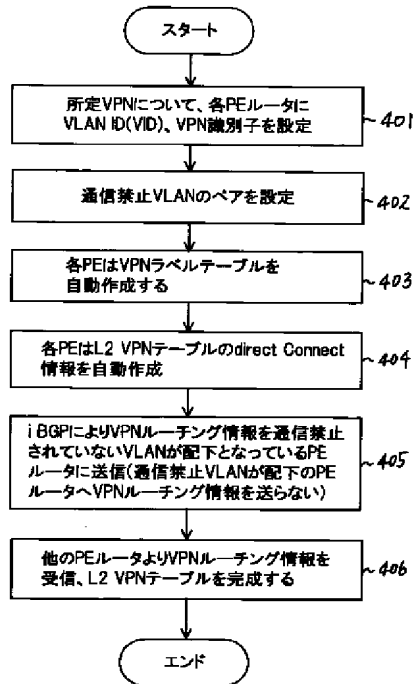


【図8】

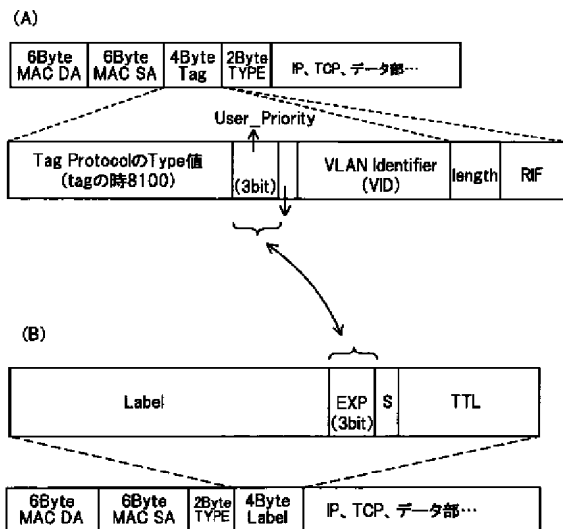
L2 OVER MPLS (VLAN over MPLS)



【図16】

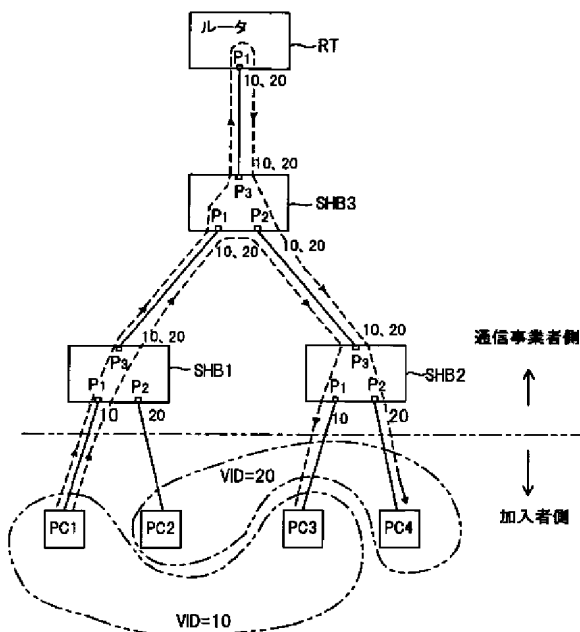
通信禁止VLANが存在する場合における
L2VPNテーブル作成処理

【図17】

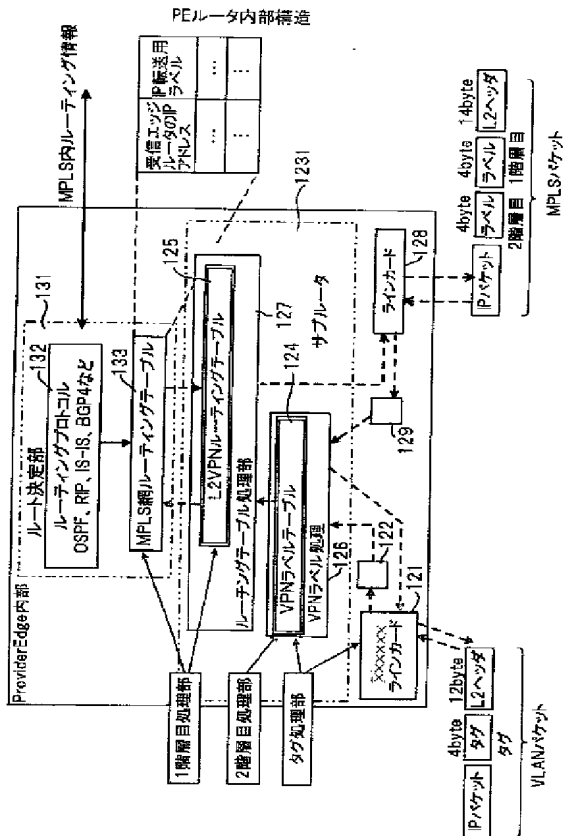
VLANにおけるユーザプライオリティとMPLSにおける
IP Precedenceの対応説明図

【図21】

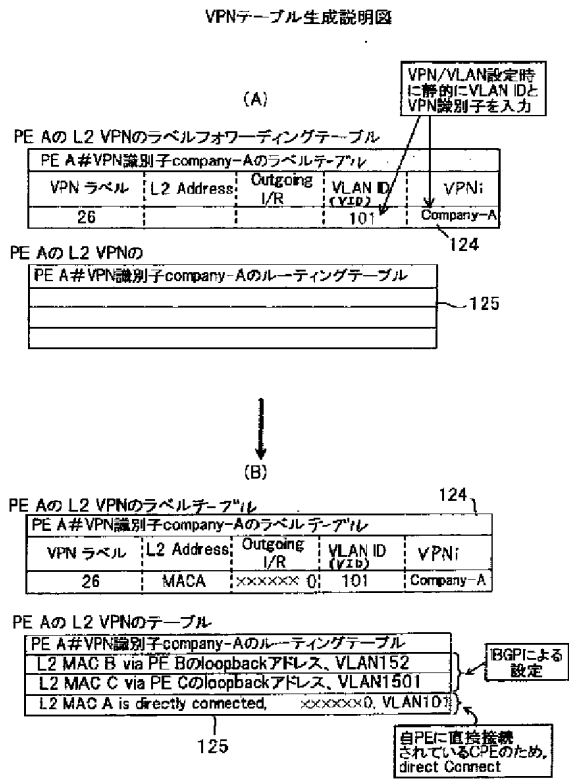
VLANの実現例



【图9】

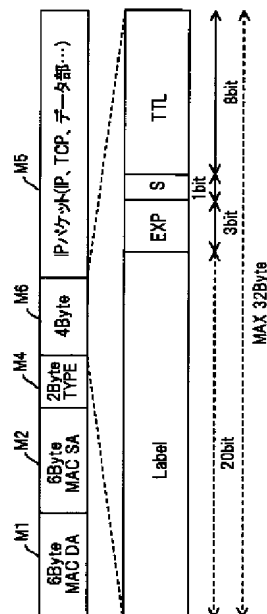


【☒ 10】



【図24】

MPLS シムヘッダの構造及び挿入位置説明図



【図 1 1】

各PEにおける企業のVPNテーブル説明図

(a)PEAにおけるA企業のVPNテーブル

#A企業のL2 VPNラベルテーブル				
VPN ラベル	OutgoingI/F	MAC	VID	VPNi
26	xxxxxxxx	MAC A	101	CompanyA

#A企業のL2VPNルーティングテーブル				
L2	MAC B	PE Bのloopbackアドレス、VLAN152		
L2	MAC C	PE Cのloopbackアドレス、VLAN1501		
L2	MAC A	directly connected, xxxxxx, VLAN101		

(b)PEBにおけるB企業のVPNテーブル

#A企業のL2 VPNラベルテーブル				
VPN ラベル	OutgoingI/F	MAC	VID	VPNi
26	xxxxxxxx	MAC B	152	CompanyA

#A企業のL2VPNテーブル				
L2	MAC B	directly connected, xxxxxx, VLAN152		
L2	MAC C	PE Cのloopbackアドレス、VLAN1501		
L2	MAC A	PE Aのloopbackアドレス、VLAN101		

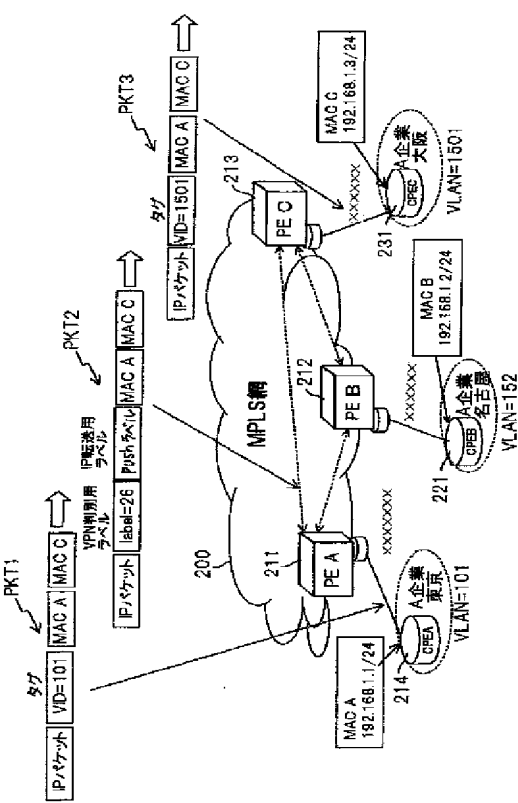
(c)PECにおけるC企業のVPNテーブル

#A企業のL2 VPNラベルテーブル				
VPN ラベル	OutgoingI/F	MAC	VID	VPNi
26	xxxxxxxx	MAC C	1501	CompanyA

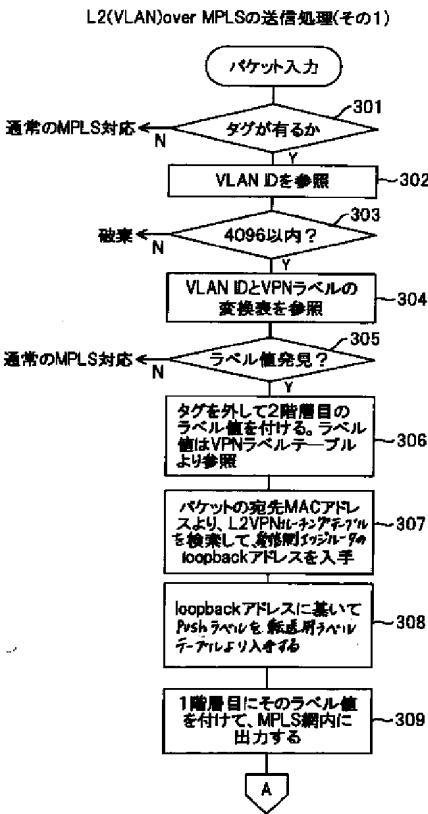
#A企業のL2VPNテーブル				
L2	MAC B	PE Bのloopbackアドレス、VLAN152		
L2	MAC C	directly connected, xxxxxx, VLAN1501		
L2	MAC A	PE Aのloopbackアドレス、VLAN101		

【図 1 2】

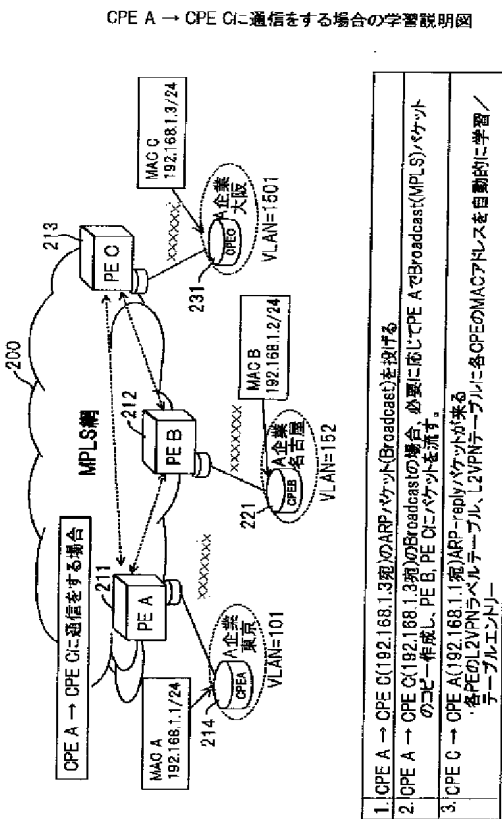
CPEA→CPEC送信説明図



【図13】

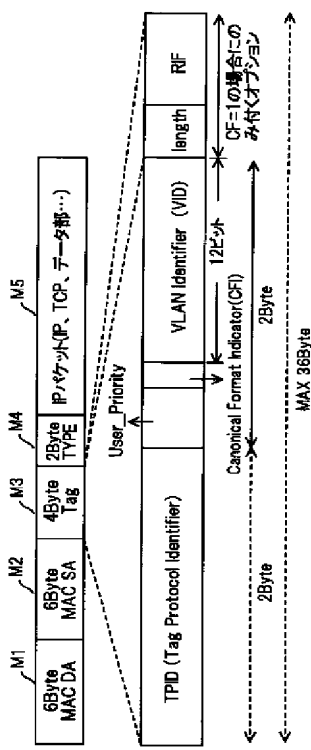


【図15】



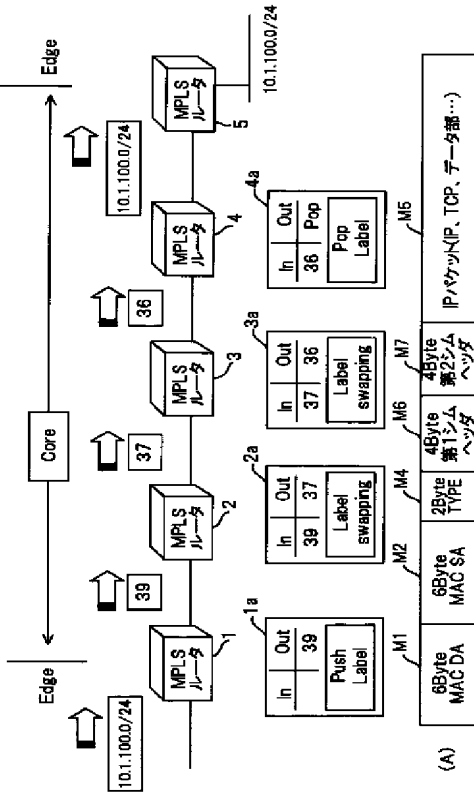
【図20】

VLAN の MACフレームフォーマット



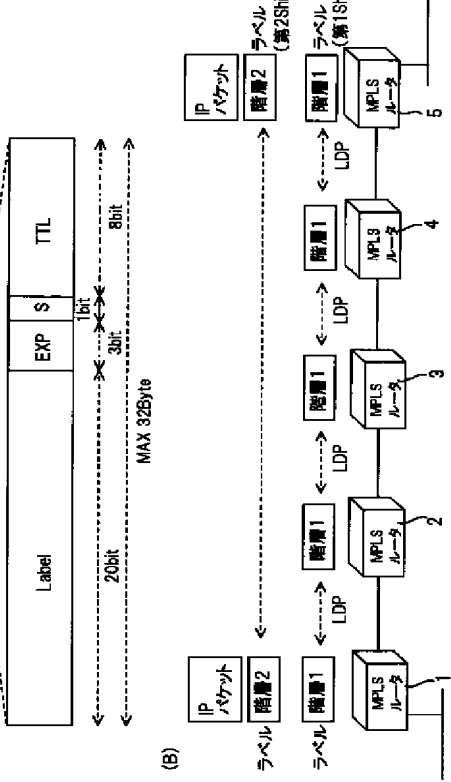
【図22】

MPLS 説明図



【図25】

シムヘッダのスタック説明図



【図27】

MPLS/VPNsの説明図

